

#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT

In re application of: **Tetsuo TAKAGI**

Serial Number: **Not Yet Assigned**

Filed: **January 4, 2001**

For: **FALSIFICATION PREVENTING APPARATUS, FALSIFICATION
PREVENTING METHOD AND RECORDING MEDIUM THEREFOR**



CLAIM FOR PRIORITY UNDER 35 U.S.C. 119

Director of Patents and Trademarks
Washington, D.C. 20231

January 4, 2001

Sir:

The benefit of the filing date of the following prior foreign application is hereby requested for the above-identified application, and the priority provided in 35 U.S.C. 119 is hereby claimed:

Japanese Appln. No. 2000-250006, filed on August 21, 2000

In support of this claim, the requisite certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the applicant has complied with the requirements of 35 U.S.C. 119 and that the Patent and Trademark Office kindly acknowledge receipt of said certified copy.

In the event that any fees are due in connection with this paper, please charge our Deposit Account No. 01-2340.

Respectfully submitted,
ARMSTRONG, WESTERMAN, HATTORI
McLELAND & NAUGHTON, LLP

Mel R. Quintos
Reg. No. 31,898

Atty. Docket No.: 001738
Suite 1000, 1725 K Street, N.W.
Washington, D.C. 20006
Tel: (202) 659-2930
Fax: (202) 887-0357
MRQ/yap

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

1c918 U.S. PTO
09/153622
01/04/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

2000年 8月21日

出願番号
Application Number:

特願2000-250006

出願人
Applicant(s):

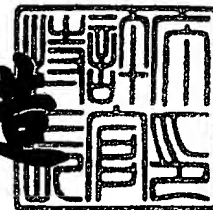
株式会社ネットワークドック

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年11月17日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3095011

【書類名】 特許願

【整理番号】 P-13965

【特記事項】 特許法第 3 0 条第 1 項の規定の適用を受けようとする特
許出願

【提出日】 平成12年 8月21日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明の名称】 改ざん防止装置及びその方法

【請求項の数】 5

【発明者】

【住所又は居所】 大阪府大阪市淀川区西中島 6 丁目 1 番 3 号 アストロ新
大阪第 2 ビル エムオーテックス株式会社内

【氏名】 高木 哲男

【特許出願人】

【識別番号】 500358825

【氏名又は名称】 株式会社ネットワークドック

【代理人】

【識別番号】 100076233

【弁理士】

【氏名又は名称】 伊藤 進

【手数料の表示】

【予納台帳番号】 013387

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 改ざん防止装置及びその方法

【特許請求の範囲】

【請求項 1】 インターネット上に公開するページを格納する公開用記録領域と、

前記公開用記録領域に格納されている情報のバックアップ情報を格納するバックアップ記録領域と、

前記公開用記録領域に対する書込み命令を検出する監視手段と、

前記監視手段によって前記公開用記録領域に対する書込み命令が検出されると、前記バックアップ記録領域に格納されているバックアップ情報を前記公開用記録領域にコピーするコピー手段とを具備したことを特徴とする改ざん防止装置。

【請求項 2】 前記公開用記録領域に格納されている情報を更新するための更新用記録領域を更に有し、

前記コピー手段は、前記更新用記録領域に格納されている情報が更新されると、前記更新用記録領域に格納されている情報を前記公開用記録領域及び前記バックアップ記録領域にコピーすることを特徴とする請求項 1 に記載の改ざん防止装置。

【請求項 3】 前記更新用記録領域の更新時にユーザー認証を実行する認証手段を更に具備したことを特徴とする請求項 2 に記載の改ざん防止装置。

【請求項 4】 インターネット上に公開するページを格納する公開用記録領域に対する書込み命令を検出する手順と、

前記公開用記録領域に対する書込み命令を検出すると、前記公開用記録領域に格納されている情報のバックアップ情報を格納するバックアップ記録領域から前記バックアップ情報を読み出して前記公開用記録領域にコピーする手順とを具備したことを特徴とする改ざん防止方法。

【請求項 5】 ユーザー認証が実行されると、前記公開用記録領域及び前記バックアップ記録領域の情報を更新可能にする手順を更に具備したことを特徴とする請求項 4 に記載の改ざん防止方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、インターネット上のWebサーバに好適な改ざん防止装置及びその方法に関する。

【0002】

【従来の技術】

近年、インターネットが急速に普及してきている。特に、Webサーバへのアクセス（Webアクセス）は、インターネット上における各種情報の公開及び取得を容易にしており、広く普及している。インターネットのWWW（World Wide web）上における情報の公開先を通常「ホームページ」と呼び、このホームページをWebサーバ上に格納することによって、情報の公開が行われる。

【0003】

ユーザーは、インターネット上に接続されたパソコン上のWebブラウザソフトを利用して、ホームページのアドレスであるURLを指定することで、Webサーバにアクセスして所望の情報（ページ）をダウンロードして表示させることができる。

【0004】

しかしながら、近年、Webサーバ上のホームページに不正アクセスし、改ざん等を行うハッカー、クラッカー等が増加してきた。これらの不正侵入者は、例えば、Webサーバのセキュリティホールを利用してWebサーバに不正に侵入し、ホームページ内の情報を改ざんする。

【0005】

このような不正侵入者の不正アクセスを未然に防ぐために、情報公開者側がファイアウォールを構築することが考えられる。しかしながら、セキュリティレベルを高く設定するためには、ファイアウォールを高度に構築する必要があり、また、セキュリティ管理も煩雑である。しかも、一端ファイアウォールを越えて不正侵入されると、Webサーバの改ざん等を阻止することができない。

【0006】

そこで、ファイルが改ざんされたことを、チェックサムの計算等によって検出

して、管理者に通知するシステムが考えられている。この手法では、ファイル全体の特徴を抽出して小さなビット列に変換した値をチェックサムとして用いている。元のファイルのチェックサムの値を監視することで不正な改ざんを検知するのである。

【0007】

【発明が解決しようとする課題】

しかしながら、ファイルのチェックサムを監視して不正な改ざんを検知する手法では、監視のための演算及びチェックサムの記録のために極めて大きなCPU能力及び記録容量を必要とするという問題点があった。

【0008】

本発明はかかる問題点に鑑みてなされたものであって、大きなCPU能力及び記録容量を必要とすることなく、改ざん直後に元のファイルに自動的に戻すことを可能にすることにより改ざんを防止することができる改ざん防止装置及びその方法を提供することを目的とする。

【0009】

【課題を解決するための手段】

本発明の請求項1に係る改ざん防止装置は、インターネット上に公開するページを格納する公開用記録領域と、前記公開用記録領域に格納されている情報のバックアップ情報を格納するバックアップ記録領域と、前記公開用記録領域に対する書込み命令を検出する監視手段と、前記監視手段によって前記公開用記録領域に対する書込み命令が検出されると、前記バックアップ記録領域に格納されているバックアップ情報を前記公開用記録領域にコピーするコピー手段とを具備したものであり、

本発明の請求項4に係る改ざん防止方法は、インターネット上に公開するページを格納する公開用記録領域に対する書込み命令を検出する手順と、前記公開用記録領域に対する書込み命令を検出すると、前記公開用記録領域に格納されている情報のバックアップ情報を格納するバックアップ記録領域から前記バックアップ情報を読み出して前記公開用記録領域にコピーする手順とを具備したものである。

【0010】

本発明の請求項1においては、インターネット上に公開するページを格納する公開用記録領域とバックアップ情報を格納するバックアップ記録領域とを有する。公開用記録領域に対して書込み命令が発生すると、監視手段はこの書込み命令を検出する。コピー手段は、監視手段によって書込み命令が検出されると、バックアップ記録領域に格納されているバックアップ情報を公開用記録領域にコピーし、改ざんされた公開用記録領域を自動的に修復する。

【0011】

本発明の請求項4において、公開用記録領域に対する書込み命令が発生するとこの書込み命令が検出される。公開用記録領域の内容を検査することなく公開用記録領域の改ざんが検出される。公開用記録領域に対する書込み命令が検出されると、バックアップ記録領域に格納されているバックアップ情報を公開用記録領域にコピーする。これにより、改ざんされた公開用記録領域が自動的に修復される。

【0012】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態について詳細に説明する。図1は本発明に係る改ざん防止装置の一実施の形態を示すブロック図である。また、図2は改ざん防止システムを説明するための説明図である。

【0013】

図2において、インターネット11上には複数のパソコン12及び各種インターネット端末13が接続されている。情報公開者のネットワーク14は、ルータ15を介してインターネット11に接続されている。ルータ15とWebサーバ17との間にはファイアーウォール16が設けられており、ファイアーウォール16は、インターネット11上からのWebサーバ17への不正アクセスを防止することができるようになっている。

【0014】

例えば、ファイアーウォール16は、HTTPプロトコロ等のリクエストについてはWebサーバ17に与え、そのレスポンスをインターネット11上に出

する。しかし、ファイアーウォール16は、その他の許可しないプロトコル、サーバ及び端末等のアクセスを禁止することができるようになっている。ファイアーウォール16は、アプリケーション毎のアクセス制限を可能にする。

【0015】

Webサーバ17は、例えば、OS（オペレーションシステム）としてWindows NT（登録商標）を採用し、Webアクセスに応答した処理を実行することができるようになっている。即ち、Webサーバ17は、HTTPプロトコル等のリクエストに응答して、指定されたファイルをレスポンスとして送出する。

【0016】

本実施の形態においては、Webサーバ17は、公開用ディレクトリ18にホームページを格納すると共に、この公開用ディレクトリ18のバックアップ用の複数のバックアップディレクトリ19, 19, ...を有している。Webサーバ17は、所定時間毎に、公開用ディレクトリ18とバックアップディレクトリ19, 19...との同期をとっており、公開用ディレクトリ18が改ざんされると、自動的にバックアップディレクトリ19の内容によって公開用ディレクトリ18を更新することができるようになっている。

【0017】

また、Webサーバ17は、Webページ更新用ディレクトリ21を有しており、Webページ更新用ディレクトリ21の内容で公開用ディレクトリ18及びバックアップディレクトリ19を更新することができるようになっている。ホームページの本来の書換え時には、Webページ更新用ディレクトリ21を書き換えることで、ホームページを更新して公開することが可能である。

【0018】

図1は図2のWebサーバ17を構成するコンピュータ上に組込まれる改ざん防止装置の具体的な構成を示すブロック図である。

【0019】

I/O（入出力部）8は図2のファイアーウォール16に接続される。入力装置7は、キーボード等によって構成され、ユーザー操作に基づく信号を制御部1

に出力して、制御部1に対して各種の指示を行う。

【0020】

制御部1は、Windows NT等のOSや、サーバソフト等によって実現されるものであり、入力装置7からの信号に基づいて動作して、各部を制御するようになっている。

【0021】

記録部2は、ハードディスク等によって構成されており、図2の公開用ディレクトリ、バックアップディレクトリ及びWebページ更新用ディレクトリ等を格納する領域を有する。書込み読出し制御部3は、記録部2の書込み及び読出しを制御する。記録部2は、書込み読出し制御部3に制御されて、制御部1からの情報を記録すると共に、記録した情報を読出して制御部1に与えるようになっている。

【0022】

制御部1は、I/O8からホームページのリクエストが入力されると、書込み読出し制御部3を制御して、記録部2の公開用ディレクトリに記録されているホームページを読出し、I/O8を介してレスポンスとしてインターネット11に送出するようになっている。

【0023】

本実施の形態においては、書込み読出し制御部3が公開用ディレクトリに対して書込み指示を与えたか否かを検出する監視部4が設けられている。監視部4は、公開用ディレクトリに対して書込みが発生したことを検出して改ざん検出信号を制御部1に出力するようになっている。また、本実施の形態においては、バックアップディレクトリの内容を公開用ディレクトリにコピーするためのコピー制御部6も設けられている。コピー制御部6は、制御部1に制御されて、書込み読出し制御部3に指示を与えてデータのコピーを行うようになっている。

【0024】

制御部1は、監視部4から改ざん検出信号が入力されると、コピー制御部6を制御して、バックアップディレクトリの内容を公開用ディレクトリにコピーさせるようになっている。また、コピー制御部6は、Webページ更新用ディレクトリ

りに対して更新が行われると、制御部 1 に制御されて、Web ページ更新用ディレクトリの内容をバックアップディレクトリ及び公開用ディレクトリにコピーするようになっている。

【0025】

なお、コピー制御部 6 によるコピー動作時には、監視部 4 の監視は無効にされるようになっている。

【0026】

また、制御部 1 は、改ざん検出信号が入力されると、I/O 8 を介してネットワーク 14 上の図示しない管理者用コンピュータに対して、改ざんが発生したことを通知すると共に、図示しない表示部に対して改ざんが発生したことを示す表示を表示させることができるようになっている。

【0027】

認証部 5 は、書込み読出し制御部 3 によって、記録部 2 の Web ページ更新用ディレクトリ及びバックアップディレクトリに対する書込み時には、ユーザー認証を要求するようになっている。制御部 1 は、認証部 5 によってユーザー認証が要求されると、ユーザー認証が要求されていることを表示部等によって表示させ、例えば、I/O 8 を介して又は入力装置 7 等によって、ユーザー ID 及びパスワード等をユーザーに入力させるようになっている。認証部 5 は、ユーザー認証が行われた場合にのみ、記録部 2 への書込みを許可するようになっている。

【0028】

次に、このように構成された実施の形態の動作について説明する。

【0029】

いま、インターネット 11 上のパソコン 12 を利用可能なユーザーが、公開された Web サーバにアクセスして、ホームページの情報を取得するものとする。ユーザーはパソコン 12 上において、ブラウザソフトを起動して、ホームページの URL を入力する。パソコン 12 からのリクエストは、インターネット 11 を介して情報公開者のネットワーク 14 に伝送される。ルータ 15 はインターネット 11 を介して伝送されたリクエストを、ファイアーウォール 16 を介して Web サーバ 17 に供給する。このリクエストは、I/O 8 を介して制御部 1 に伝送

される。

【0030】

制御部1は、リクエストに応じて書込み読出し制御部3を制御し、記録部2の公開用ディレクトリに格納されているホームページの情報を読出して、I/O8からレスポンスとして送出する。このレスポンスは、ファイアーウォール16及びルータ15を介してインターネット11上に送出され、パソコン12に取込まれる。こうして、パソコン12上で起動されているブラウザソフトは、受信したレスポンスに基づいて、ホームページを表示する。こうして、インターネット11上のユーザーは、ブラウザソフト上で、情報公開者が提供するホームページを見ることができる。

【0031】

ここで、インターネット11上のユーザーが何らかの手段によってファイアーウォール16内に不正に侵入して、Webサーバ17内のホームページを改ざんするものとする。不正侵入者による書込み命令は、制御部1によって書込み読出し制御部3に供給される。読出し制御部3は、記録部2の公開用ディレクトリに対して書込みを行う。

【0032】

一方、監視部4は、書込み読出し制御部3による書込み命令を検出しており、改ざん検出信号を制御部1に出力する。そうすると、制御部1は、コピー制御部6に対して、バックアップディレクトリの内容を公開用ディレクトリにコピーさせる。監視部4が比較的短い周期で改ざんを監視することにより、極めて短時間にバックアップディレクトリによる復旧が可能である。例えば、コピー制御部6は、改ざんが開始された後の数ミリ秒程度で、バックアップディレクトリの内容のコピーを開始することができる。

【0033】

従って、この場合には、不正侵入者による改ざんが行われると略同時に元のデータへの復旧が行われることになり、他の一般ユーザのパソコン上には、改ざんが行われていない状態のホームページが表示される。なお、不正侵入者による改ざんの検出から、所定時間後に、データを元のデータに復旧させるようにしても

よい。

【0034】

監視部4は、公開用ディレクトリに対する書込み命令を検出することで改ざんの有無を監視しており、公開用ディレクトリの解析等を行っておらず、改ざん検出のために大容量の記録部は不要であり、また、高いCPU能力も不要である。

【0035】

監視部4は、例えばWindows NTの機能を用いて実現することができ、制御部1は、改ざん検出信号によって割り込み命令を発生して、コピー制御を行うことで、改ざんの監視及びデータの復旧を容易に且つ迅速に行うことができる。

【0036】

次に、情報公開者自らが公開用ディレクトリを更新するものとする。この場合には、情報公開者は、例えば入力装置7によって公開用ディレクトリの更新を指示する。制御部1は、更新指示を書込み読出し制御部3に出力して、Webページ更新用ディレクトリの書込みを行う。この書込みに際して、認証部5は、ユーザー認証を要求する。制御部1は、ユーザー認証のための表示を表示部に表示させる。ユーザーは、ユーザー認証のためのID及びパスワード等を入力装置7によって入力する。認証部5は、ユーザの入力操作によるID及びパスワードが予め登録されている情報と一致している場合にのみ、Webページ更新用ディレクトリの書込みを許可する。これにより、不正侵入者によるWebページ更新用ディレクトリの書込みは阻止される。なお、不正侵入者によるバックアップディレクトリに対する書込みも阻止されることは同様である。

【0037】

ユーザー認証が行われると、書込み読出し制御部3は、Webページ更新用ディレクトリをユーザ操作に基づいて更新する。コピー制御部6は、Webページ更新用ディレクトリ、バックアップディレクトリ及び公開用ディレクトリの同期をとっており、Webページ更新用ディレクトリが更新されると、Webページ更新用ディレクトリの内容をバックアップディレクトリ及び公開用ディレクトリにコピーする。こうして、公開用ディレクトリの更新が行われる。

【 0 0 3 8 】

このように、本実施の形態においては、公開用ディレクトリに対する書込みを検出することで改ざんを検出しており、改ざんの検出から短時間でバックアップディレクトリの内容を公開用ディレクトリにコピーして公開用ディレクトリを改ざんから自動修復させるようになっている。これにより、大容量の記録部及び高い能力のCPUを必要とすることなく、改ざんを防止することができる。

【 0 0 3 9 】

なお、情報公開者による公開用ディレクトリの更新時には、改ざんの検出及びコピーによる自動修復機能を一時停止させるようにしてもよい。この場合には、直接公開用ディレクトリ又はバックアップディレクトリ等を更新することができる。

【 0 0 4 0 】

なお、記録部2は1つのハードディスクで構成するのではなく、複数のハードディスク或いは複数種類の記録メディアによって構成することができる。また、例えば、電気通信回線によって、他の記録メディアに記録された公開用ディレクトリ、バックアップディレクトリ及びWebページ更新用ディレクトリ間で同期をとりコピーを行うようにしてもよいことは明らかである。

【 0 0 4 1 】

【発明の効果】

以上説明したように本発明によれば、大きなCPU能力及び記録容量を必要とすることなく、改ざん直後に元のファイルに自動的に戻すことを可能にすることにより改ざんを防止することができるという効果を有する。

【図面の簡単な説明】

【図1】

本発明に係る改ざん防止装置の一実施の形態を示すブロック図。

【図2】

改ざん防止システムを説明するための説明図。

【符号の説明】

1 …制御部、 2 …記録部、 3 …書込み読出し制御部、 4 …監視部、 5 …認証

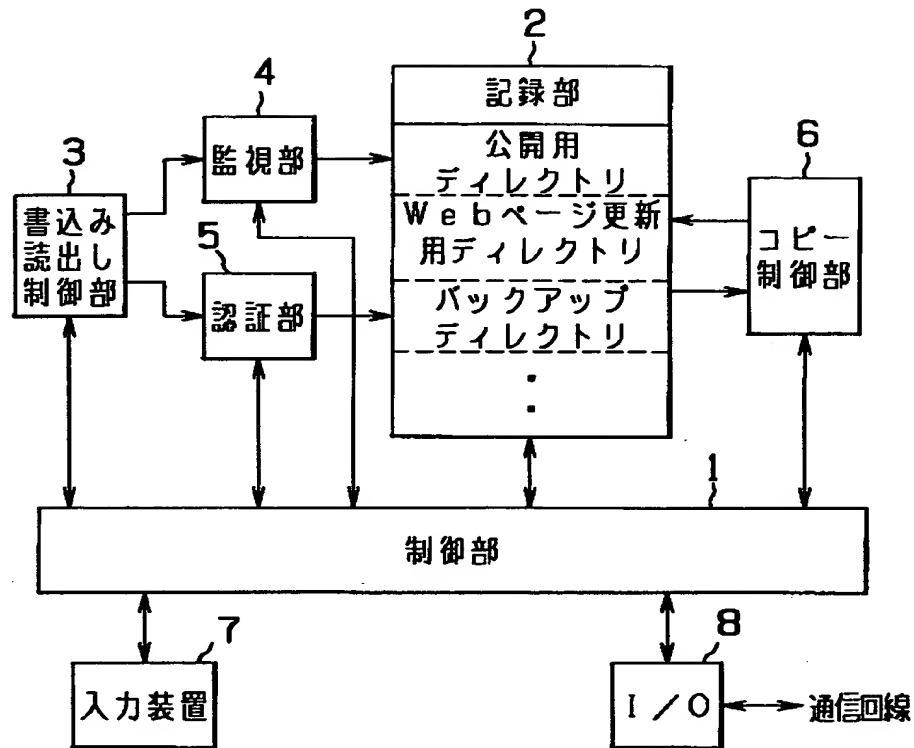
部、6…コピー制御部、7…入力装置、8…I/O。

代理人 弁理士 伊 藤 進

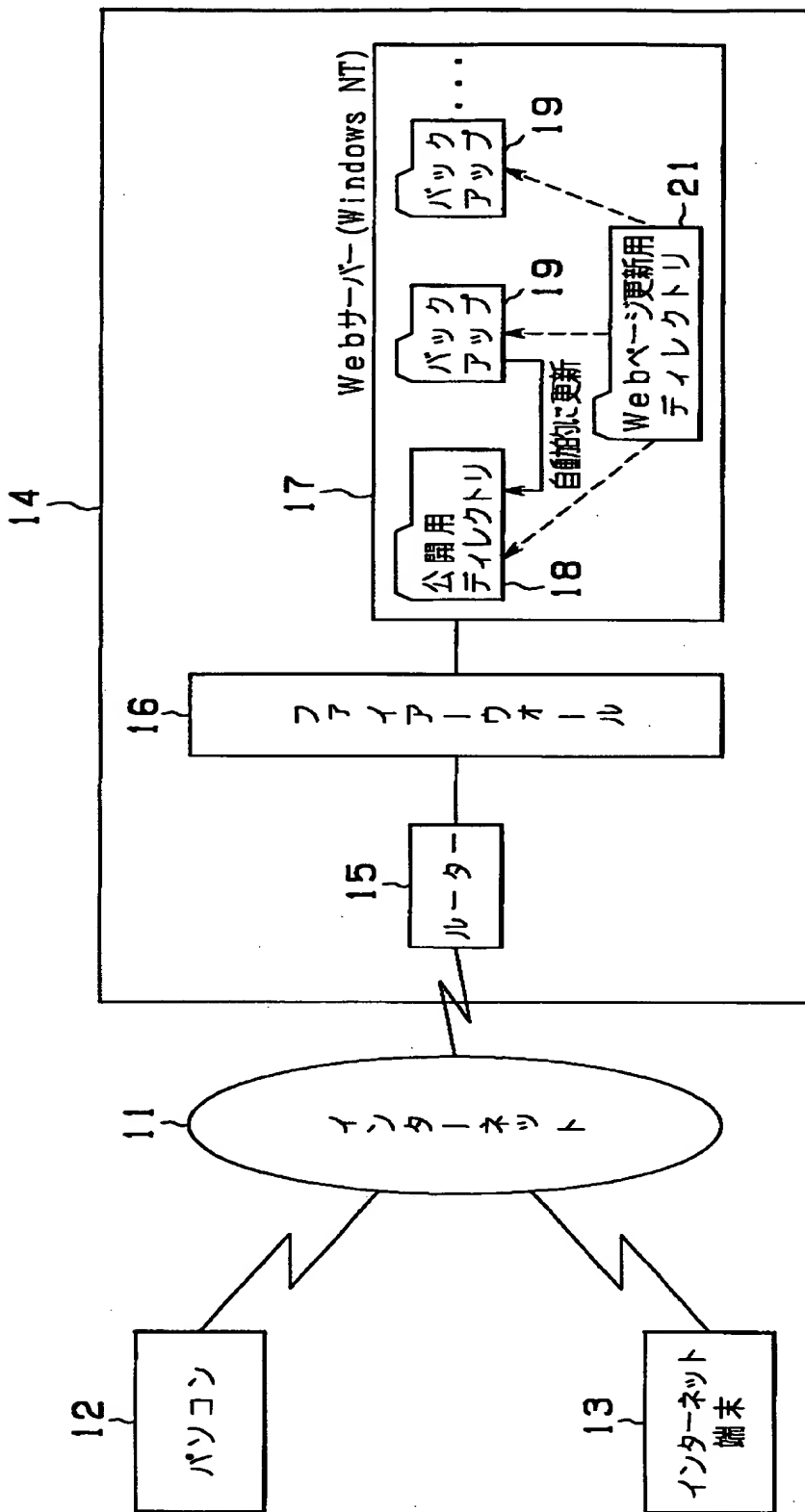
【書類名】

図面

【図 1】



【図2】



【書類名】 要約書

【要約】

【課題】 W e b ページの改ざんを防止する。

【解決手段】 監視部 4 は、書込み読出し制御部 3 による記録部 2 の公開用ディレクトリに対する書込み命令を検出する。制御部 1 は、監視部 4 から改ざん検出信号が入力されると、コピー制御部 6 を制御して、バックアップディレクトリに格納されている情報を読出して公開用ディレクトリにコピーする。これにより、公開用ディレクトリの改ざんが防止される。書込み命令の検出によって改ざんを検出しており、改ざんの検出に大容量の記録装置及び高い C P U 能力を必要としない。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [500358825]

1. 変更年月日 2000年 7月25日

[変更理由] 新規登録

住 所 東京都中央区日本橋浜町3丁目19番2号
氏 名 株式会社ネットワークドック